Best Practices in Wireless Networks

Presented by:

The Office of Legislative Audits

Introduction

- **Presenter:** Tony Vaccare, CPA, CISA
  - Senior Information Systems Auditor
  - Primarily Responsible for Performing Network Audits of State Agencies
  - Performing Information Systems Audits for over 5 years

Introduction

- What we have seen in our wireless network audits:
  - **Size:** Installations with up to 250 access points
  - **Uses:** Internet and e-mail connectivity
  - There are not many sizeable wireless networks at State agencies

Introduction

- **Problems:**
  - Encryption and/or VPNs are not used
  - Ad-hoc wireless networks exist without the IT Department's authorization and support
  - Indirect access to critical systems can be attained via weak security on wireless and wired network devices
  - Free Internet access!

Wireless Networking Background

- **Characteristics of Wireless Technology:**
  - Broadcast networks
  - Easy to deploy
  - Easy to join
  - Inherently insecure (communications sent through the air)
  - Susceptible to “sniffing”
  - Designed around the IEEE 802.11 standards (802.11b, 802.11a, 802.11g)

Wireless Networking Background

- **Characteristics of Wireless Technology (Cont.):**
  - By default, relies on physical and data link layers of the OSI model
  - Wireless devices are cheap and easy to install
  - Designed to support transient, intermittent users
  - Convenience vs. security

Wireless LANS (WLANs)

- Infrastructure Mode vs. Ad-hoc Mode
  - **Infrastructure Mode** – wireless clients communicate with central access points
  - **Ad-hoc Mode** – wireless clients communicate with other wireless clients without an intervening access point

Wireless LANS (WLANs)

- Objectives of WLANs:
  - Connect systems and devices in an office or campus environment
  - Connect to the Internet
- The distance range of wireless devices is typically in terms of hundreds of feet and transfer rates are typically between 2 - 54 Megabits/second

Wireless LANS (WLANs)

- Wireless devices have a high power consumption
- WEP (Wired Equivalent Privacy) and WEP2 are flawed encryption methods
- The Extensible Authentication Protocol (EAP), available under 802.1x, is a far more secure authentication method

Wireless LANS (WLANs)

- VPNs
  - Opens up greater possibilities for authentication and encryption
  - However, VPN protocols are not always compatible with certain wireless devices, particularly access points and PDAs

Basic WLAN Security Concerns

- **Authentication:**
  - Open System Authentication
  - WEP2
  - Shared-key Authentication
  - 802.1x Authentication (EAP)

Basic WLAN Security Concerns

- **Confidentiality:**
  - WEP and WEP2 are better than nothing
  - Use a VPN!

Basic WLAN Security Concerns

- **Integrity:**
  - WEP and WEP2 are susceptible to man-in-the-middle attacks and session hijacking
  - Use a VPN!

Risks of Wireless Networks

- Free Internet access to unauthorized individuals ("war drivers")
- A potential back door into the network
  - Privilege Escalation
  - Another potential vulnerability to viruses, trojans, worms, etc.
- Privacy of communications, especially sensitive data

Preferred Wireless Network Practices

- Create a specific wireless networking security policy
- Maintain an inventory of wireless devices, primarily access points
- Perform periodic audits to detect rogue access points and/or ad-hoc wireless networks (e.g., AirMagnet)
- If possible, restrict wireless users to non-critical systems, e-mail, and the Internet

Preferred Wireless Network Practices

- Access Points
  - Use strong passwords (i.e., according to DBM's requirements)
  - Use a secure channel (e.g., SSL) to manage access points
  - Patch and upgrade access point software as needed
  - Always treat the wireless network as an external, third-party, untrusted network

Preferred Wireless Network Practices

- Convenience vs. Security
  - Require all wireless users to go through a gateway and encrypt communications with a secure protocol
  - WEP is not acceptable, use a VPN
  - Use a backend authentication server (e.g., RADIUS) in a secure environment
  - Employ 802.1x technology (dynamic key management, token cards, Kerberos, and/or PKI)

END OF PRESENTATION

Tony Vaccare
Office of Legislative Audits
rvaccare@ola.state.md.us